

Obsah dokumentu.

Úvod.....	2
Klíčové důvody, proč se zabývat propojením AI a GDPR.....	2
Co podnikla EU: právní rámec a nové instituce.....	2
Evropský úřad pro umělou inteligenci (AI Office).....	3
Pakt AI: dobrovolná iniciativa a komunita praxe.....	3
Co si musí firmy pohlídat.....	3
Zakázané praktiky AI v EU – podrobný rozbor.....	4
1. Manipulace pomocí podprahových technik.....	4
2. Zneužívání zranitelnosti jednotlivců.....	4
3. Sociální skórování.....	4
4. Prediktivní policejní algoritmy založené na osobnosti.....	4
5. Masový sběr obličejových dat.....	5
6. Rozpoznávání emocí na pracovišti a ve školách.....	5
7. Biometrická kategorizace podle citlivých charakteristik.....	5
8. Biometrická identifikace v reálném čase.....	5
Obecné zásady transparentnosti AI.....	6
Zásady transparentnosti AI podle oblastí.....	7
Osnovy posouzení vlivu na ochranu osobních údajů (DPIA).....	8
Přehled klíčových webových stránek.....	10
Nařízení EU a Pakt AI.....	11
NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2024/1689.....	11
Pakt AI.....	11
Umělá inteligence.....	11
Evropský úřad pro umělou inteligenci.....	11

Úvod

Rozvoj umělé inteligence (AI) otevírá nové možnosti pro automatizaci, efektivitu a inovace napříč všemi odvětvími. Současně však přináší i nové výzvy v oblasti ochrany osobních údajů a základních práv jednotlivců. Právě proto je klíčové, aby organizace věnovaly pozornost vztahu mezi AI a Obecným nařízením o ochraně osobních údajů (GDPR), které tvoří základní právní rámec pro nakládání s osobními údaji v EU.

Klíčové důvody, proč se zabývat propojením AI a GDPR

Umělá inteligence zpracovává obrovské množství dat, z nichž mnohá mohou být osobní, citlivá nebo jinak chráněná. GDPR stanovuje, že pro jakékoli zpracování těchto údajů musí být jasně definován právní základ – například souhlas, smlouva nebo oprávněný zájem. AI systémy proto musí být navrženy tak, aby zpracovávaly pouze nezbytné údaje a respektovaly zásadu minimalizace. Dále platí povinnost transparentnosti – subjekty údajů musí být informovány o způsobu, jakým jsou jejich data zpracovávána, a mají právo požadovat lidský zásah v případě, že dochází k automatizovanému rozhodování. Zásadním rizikem je automatizované rozhodování bez lidského dohledu, například při náborech zaměstnanců, hodnocení úvěruschopnosti nebo při práci s biometrickými údaji. GDPR v článku 22 přímo zakazuje rozhodování, které má významné právní důsledky, bez možnosti lidského přezkumu, pokud nejsou splněny výjimečné podmínky. Firmy musí být připraveny prokázat, že jejich AI systémy respektují práva subjektů údajů – tedy právo na přístup, opravu, výmaz, přenositelnost údajů nebo vznesení námítky. AI musí být také technicky navržena s důrazem na soukromí („privacy by design“) a bezpečnost („by default“), včetně zavedení přístupových kontrol, šifrování a pravidelných auditů. V neposlední řadě je důležité vést podrobnou dokumentaci o tom, jak AI systém funguje, jaká data používá a jak je spravuje.

Co podnikla EU: právní rámec a nové instituce

Evropská unie odpověděla na výzvy spojené s AI přijetím vůbec prvního komplexního právního rámce pro umělou inteligenci – Nařízení (EU) 2024/1689 o umělé inteligenci, známého jako AI Act. Toto nařízení vstoupilo v platnost 1. srpna 2024 a jeho jednotlivá ustanovení se budou postupně uplatňovat až do srpna 2026. AI Act zavádí přístup založený na posouzení rizik. Rozlišuje čtyři úrovně rizika: nepřijatelné, vysoce rizikové, omezené a minimální riziko. Nepřijatelné aplikace, například sociální skórování nebo manipulace zranitelných osob, jsou zcela zakázány. Vysoce rizikové systémy (např. v oblasti zdravotnictví, dopravy, HR nebo biometrie) musejí projít posouzením shody, zavést řízení rizik, zajistit transparentnost, lidský dohled a kybernetickou bezpečnost. Nařízení také specifikuje povinnosti pro tzv. generativní AI – například označování výstupů vytvořených umělou inteligencí a opatření proti deep fakes. AI Act v neposlední řadě doplňuje GDPR, nikoliv ho nahrazuje – oba právní rámce se navzájem posilují, zejména v oblastech, jako jsou vysvětlitelnost algoritmů a ochrana základních práv.

Evropský úřad pro umělou inteligenci (AI Office)

Pro dohled nad implementací a koordinací AI Actu byl zřízen Evropský úřad pro umělou inteligenci (European AI Office). Tento úřad funguje jako centrum odbornosti, regulační autorita a hlavní vykonavatel politiky EU v oblasti AI. Podporuje členské státy, vyvíjí kodexy praxe, vydává metodiky pro klasifikaci modelů a hodnotí systémová rizika spojená s tzv. všeobecnými modely AI (např. LLM). Úřad má rovněž za úkol spolupracovat s mezinárodními partnery, koordinovat Evropskou radu pro umělou inteligenci a dohlížet na transparentnost, bezpečnost a shodu systémů AI s právními předpisy EU.

Webová stránka: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>

Pakt AI: dobrovolná iniciativa a komunita praxe

Součástí příprav na implementaci AI Actu je i tzv. Pakt o umělé inteligenci (AI Pact). Tato dobrovolná iniciativa Evropské komise vyzývá firmy a instituce, aby ještě před plnou platností zákona začaly aplikovat jeho zásady v praxi. Pakt má dvě části. První se zaměřuje na sdílení zkušeností, školení, best practices a vytváření sítě organizací, které se chtějí zapojit do odpovědného vývoje AI. Druhá část podporuje dobrovolné závazky – firmy se veřejně zavazují ke konkrétním krokům, jako je identifikace vysoce rizikových systémů, zavedení etických rámců a školení zaměstnanců v oblasti AI a datové gramotnosti. AI Pact podporuje důvěryhodnost, proaktivní přístup a usnadňuje přechod na nové regulační podmínky. Pro firmy to zároveň znamená viditelný signál vůči partnerům, investorům a veřejnosti, že berou odpovědné používání AI vážně.

Co si musí firmy pohlídat

Firmy, které chtějí využívat AI legálně a důvěryhodně, musejí zohlednit nejen technickou efektivitu systémů, ale i právní rámec a etické aspekty jejich použití. Klíčové oblasti pozornosti zahrnují výběr právního základu zpracování údajů, transparentnost algoritmů, lidský dohled nad automatizací, řízení rizik a testování systémů, zabezpečení dat a dokumentaci rozhodovacích procesů. Dodržování GDPR a AI Actu není jen povinnost – je to strategická výhoda. Umožňuje firmám inovovat s důvěrou, chránit své klienty i sebe a být součástí etického technologického rozvoje, který respektuje práva a hodnoty moderní demokratické společnosti.

Zakázané praktiky AI v EU – podrobný rozbor

1. Manipulace pomocí podprahových technik

Jedná se o používání takových metod, které ovlivňují rozhodování jednotlivce bez jeho vědomé kontroly. AI například může využít neuromarketingové přístupy – jako jsou neviditelné vizuální nebo zvukové podněty – k tomu, aby podvědomě ovlivnila nákupní chování nebo změnila postoje osoby vůči určitému produktu, službě nebo politickému postoji.

Příklad: Chatbot, který vkládá do odpovědí frekvenčně vnímatelné signály, které zvyšují pocity důvěry nebo strachu, aniž by si toho uživatel byl vědom.

Právní základ: EU AI Act čl. 5(1)(a); GDPR čl. 5

2. Zneužívání zranitelnosti jednotlivců

Týká se využívání AI systémů k manipulaci s chováním osob, které jsou kvůli věku, zdravotnímu stavu nebo sociální situaci méně schopné se bránit. AI by například neměla navrhopvat rizikové půjčky lidem ve finanční tísní nebo nabízet zboží dětem prostřednictvím her s psychologicky navrženým tlakem.

Příklad: Mobilní aplikace pro děti, která algoritmicky navrhuje nákup herních doplňků ve chvíli, kdy dítě ztratí hru a je emocionálně oslabené.

Právní základ: EU AI Act čl. 5(1)(b); GDPR čl. 6 a čl. 9

3. Sociální skórování

Zákaz se vztahuje na vytváření systémů, které posuzují důvěryhodnost nebo chování osob a podle toho určují jejich přístup k veřejným nebo soukromým službám. Tento zákaz reaguje na praktiky podobné těm, které se objevují v Číně, kde lidé získávají či ztrácejí práva podle algoritmicky vyhodnoceného 'skóre'.

Příklad: Systém, který monitoruje účast občana na protestech nebo jeho aktivitu na sociálních sítích a podle toho omezuje jeho možnost cestování nebo zaměstnání.

Právní základ: EU AI Act čl. 5(1)(c); GDPR čl. 22

4. Prediktivní policejní algoritmy založené na osobnosti

AI systémy nesmí předpovídat pravděpodobnost spáchání trestného činu pouze na základě chování, vzhledu nebo jiných osobnostních znaků. Takový přístup by vedl k tzv. profilování a potenciálním předsudkům, diskriminaci a neopodstatněnému sledování občanů.

Příklad: Algoritmus, který analyzuje sociální síť a psychologické testy ke stanovení, kdo by mohl být 'budoucím pachatelem'.

Právní základ: EU AI Act čl. 5(1)(d); GDPR čl. 9 a 22

5. Masový sběr obličejových dat

Organizace nesmí automaticky skenovat, shromažďovat a analyzovat fotografie obličejů ze sociálních sítí, kamerových záznamů nebo jiných veřejných zdrojů za účelem vytváření databází pro rozpoznávání osob.

Příklad: Startup, který bez svolení sbírá fotky z Instagramu a vytváří databázi pro identifikaci osob v obchodech nebo městských kamerách.

Právní základ: EU AI Act čl. 5(1)(e); GDPR čl. 9

6. Rozpoznávání emocí na pracovišti a ve školách

Používání AI k analýze emocí na základě výrazu tváře, hlasu nebo gesta zaměstnanců a studentů je zakázáno, pokud se nejedná o výjimečné případy jako je ochrana zdraví nebo prevence nehod.

Příklad: AI systém sledující kamery v učebně a označující 'nepozornost' studentů podle výrazů obličeje.

Právní základ: EU AI Act čl. 5(1)(f); GDPR čl. 6 a 9

7. Biometrická kategorizace podle citlivých charakteristik

AI nesmí klasifikovat lidi podle rasy, náboženství, sexuální orientace nebo politických názorů na základě biometrických údajů (např. skeny obličeje, chování).

Příklad: Systém, který na základě vzhledu přiřazuje osoby k náboženským nebo etnickým skupinám.

Právní základ: EU AI Act čl. 5(1)(g); GDPR čl. 9

8. Biometrická identifikace v reálném čase

Policie a veřejné instituce nesmí plošně sledovat veřejná prostranství pomocí AI pro rozpoznávání obličejů v reálném čase – výjimky platí pouze při velmi závažných událostech.

Příklad: Použití AI kamer na letištích k automatickému sledování všech cestujících bez konkrétního důvodu.

Právní základ: EU AI Act čl. 5(1)(h); GDPR čl. 6 odst. 1 písm. e), čl. 9

Shrnutí

Nařízení Evropské unie o umělé inteligenci (EU AI Act) definuje jasný rámec pro ochranu základních práv a svobod občanů v souvislosti s používáním systémů umělé inteligence. V rámci tohoto nařízení byly určeny praktiky, které jsou v EU zcela zakázány, protože představují nepřijatelné riziko pro lidskou důstojnost, soukromí a rovnost.

Tyto zákazy odrážejí snahu EU o etické, bezpečné a lidsky zaměřené používání AI, které nebude nástrojem diskriminace, manipulace nebo nelegitimního dohledu. Současně je zde silné propojení s pravidly ochrany osobních údajů podle GDPR, které nadále chrání integritu jednotlivců v digitálním prostoru.

Obecné zásady transparentnosti AI.

Tyto zásady stanoví základy transparentního, odpovědného a zákonného používání umělé inteligence (AI) v rámci činností organizace. Cílem je zajistit, aby používání AI systémů bylo v souladu s požadavky právních předpisů, zejména nařízení (EU) 2016/679 (GDPR), a respektovalo základní práva a svobody subjektů údajů.

1. Transparentnost

- a. AI systémy musí být navrženy a provozovány tak, aby bylo možné jasně sdělit, že se jedná o automatizované zpracování.

2. Lidský dohled

- a. Rozhodnutí s významným dopadem musí být pod kontrolou člověka.

3. Minimalizace údajů

- a. AI smí pracovat pouze s nezbytnými údaji.

4. Bezpečnost a důvěrnost

- a. Zajistit ochranu proti neoprávněnému přístupu.

5. Nediskriminace a spravedlnost

- a. AI nesmí diskriminovat na základě chráněných znaků.

6. Vysvětlitelnost

- a. Fungování AI musí být pochopitelné pro uživatele.

7. Dokumentace a odpovědnost

- a. vést evidenci o fungování a správě AI systému.

Zásady transparentnosti AI podle oblastí.

HR (nábor, hodnocení výkonu, interní analýzy)

Naše organizace využívá AI nástroje k podpoře procesů v oblasti náboru zaměstnanců, hodnocení výkonu a interního rozvoje.

- Účel: AI systém pomáhá předvýběrem kandidátů podle předem definovaných kritérií.
- Data: Jméno, vzdělání, profesní zkušenosti, výstupy z pohovorů.
- Rozhodování: AI poskytuje pouze podklad, konečné rozhodnutí činí člověk.
- Práva: Kandidáti mají právo na přezkum a další práva dle GDPR.

Kamerové systémy s AI

AI je integrována do kamerových systémů za účelem zvýšení bezpečnosti.

- Účel: Detekce pohybu, rozpoznávání podezřelého chování.
- Data: Záznamy z kamer, případně biometrie.
- Právní základ: Oprávněný zájem; při biometrice výslovný souhlas.
- Zásahy AI: Rozpoznání obličejů podléhá lidskému ověření.
- Práva: Informace, výmaz, námitka.

Lékaři

Zdravotnické zařízení používá AI při diagnostice a návrhu léčby.

- Účel: Analýza údajů pro diagnostiku a sledování stavu pacienta.
- Data: Dokumentace, laboratorní výsledky, anamnéza.
- Rozhodnutí činí vždy lékař, AI je podpůrný nástroj.
- Práva: Informace, oprava, výmaz, vysvětlení.

Lékárny

AI napomáhá přesnosti a individualizaci výdeje léčiv.

- Účel: Doporučení léků, varování na interakce.
- Data: Identifikace zákazníka, historie nákupů.
- Rozhodnutí o výdeji činí lékárník.
- Práva: Informace o použití AI, námitka.

Výrobní podnik

AI optimalizuje provoz, kvalitu a bezpečnost.

- Účel: Údržba, detekce vad, plánování směn.
- Data: Provozní, kamerové, přítomnost pracovníků.
- AI nerozhoduje samostatně.
- Práva: Přístup, vysvětlení, námitka

Osnovy posouzení vlivu na ochranu osobních údajů (DPIA)

DPIA – AI systém pro nábor zaměstnanců (HR)

1. Název projektu/systému: Automatizovaný náborový nástroj (AI Recruitment Tool)
2. Popis AI systému a jeho účelu: Systém využívá algoritmy strojového učení ke třídění životopisů a doporučení kandidátů na základě předem definovaných kritérií (vzdělání, zkušenosti, jazykové znalosti).
3. Kategorie subjektů údajů a typy údajů: Uchazeči o zaměstnání – jméno, kontaktní údaje, vzdělání, pracovní historie, jazykové dovednosti, výsledky testů.
4. Právní základ zpracování: Opatření před uzavřením smlouvy [čl. 6 odst. 1 písm. b) GDPR], případně souhlas [čl. 6 odst. 1 písm. a)].
5. Posouzení nezbytnosti a přiměřenosti zpracování: Zpracování je nezbytné pro efektivní správu náborového procesu, data jsou relevantní pro hodnocení způsobilosti.
6. Rizika pro práva a svobody subjektů údajů: Možnost diskriminace, netransparentnosti, chybných rozhodnutí na základě neúplných dat.
7. Opatření ke zmírnění rizik: Lidský dohled nad konečným rozhodnutím, pravidelné testování systému na bias, informační povinnost vůči uchazečům.
8. Závěr a doporučení: Rizika jsou přiměřená a zvládnutelná za podmínky pravidelného přezkumu a školení personálu.
9. Datum a osoba odpovědná za vypracování: 2025-04-16, Mgr. Ivana Novotná – HR manažerka

DPIA – AI systém pro kamerový dohled

1. Název projektu/systému: Inteligentní kamerový systém s AI pro detekci incidentů
2. Popis AI systému a jeho účelu: Kamerový systém s AI detekuje podezřelé pohyby, neoprávněné vstupy a chování mimo běžné vzorce za účelem zvýšení bezpečnosti.
3. Kategorie subjektů údajů a typy údajů: Zaměstnanci, návštěvníci – obrazový záznam, případně biometrické údaje [obličeje].
4. Právní základ zpracování: Oprávněný zájem správce [čl. 6 odst. 1 písm. f) GDPR], výslovný souhlas v případě biometricky [čl. 9 odst. 2 písm. a)].
5. Posouzení nezbytnosti a přiměřenosti zpracování: Kamery pokrývají pouze nezbytné oblasti, záznamy se uchovávají po omezenou dobu, přístup je kontrolovaný.
6. Rizika pro práva a svobody subjektů údajů: Neoprávněné sledování, únik záznamů, diskriminace při rozpoznávání obličejů.
7. Opatření ke zmírnění rizik: Omezený přístup k datům, šifrování záznamů, nezávislý audit systému a pravidelný přezkum algoritmů.
8. Závěr a doporučení: Použití AI je přípustné za podmínky striktního dodržení zásady minimalizace a zajištění informovanosti sledovaných osob.
9. Datum a osoba odpovědná za vypracování: 2025-04-16, Ing. Karel Dvořák – vedoucí oddělení bezpečnosti

DPIA – AI systém v diagnostice ve zdravotnictví

1. Název projektu/systému: Diagnostický pomocný systém založený na AI [AI Diagnostic Assistant]
2. Popis AI systému a jeho účelu: AI analyzuje laboratorní výsledky, lékařské zprávy a snímky k podpoře lékaře při stanovení diagnózy.
3. Kategorie subjektů údajů a typy údajů: Pacienti – jméno, rodné číslo, anamnéza, laboratorní výsledky, radiologické snímky, diagnózy.
4. Právní základ zpracování: Plnění právní povinnosti (čl. 6 odst. 1 písm. c)), poskytování zdravotní péče (čl. 9 odst. 2 písm. h)) GDPR.
5. Posouzení nezbytnosti a přiměřenosti zpracování: Údaje jsou nezbytné pro zdravotní péči, systém pracuje v uzavřeném bezpečném prostředí.
6. Rizika pro práva a svobody subjektů údajů: Chybné doporučení, únik zdravotních údajů, nedostatečná interpretace rozhodnutí AI.
7. Opatření ke zmírnění rizik: AI je pouze podpůrný nástroj, rozhodnutí činí lékař, veškerá data jsou pseudonymizována a přístup je auditován.
8. Závěr a doporučení: Použití systému je přiměřené a přínosné, doporučuje se pravidelné přehodnocení modelů a protokolů.
9. Datum a osoba odpovědná za vypracování: 2025-04-16, MUDr. Jana Doležalová – vedoucí lékařka

DPIA – AI systém ve výrobním podniku (prediktivní údržba a monitoring)

1. Název projektu/systému: AI systém pro prediktivní údržbu a monitoring výrobních linek
2. Popis AI systému a jeho účelu: Systém sbírá provozní data ze strojů a analyzuje je pro předvídaní poruch a zajištění plynulosti výroby.
3. Kategorie subjektů údajů a typy údajů: Zaměstnanci – ID pracovníka, pracovní směny, přítomnost u stroje (čas, lokalita), strojová data.
4. Právní základ zpracování: Oprávněný zájem správce (čl. 6 odst. 1 písm. f)) GDPR).
5. Posouzení nezbytnosti a přiměřenosti zpracování: Údaje o pracovní přítomnosti jsou zpracovávány pouze v nezbytném rozsahu pro účely bezpečnosti a efektivity.
6. Rizika pro práva a svobody subjektů údajů: Sledování zaměstnanců bez dostatečné informovanosti, zneužití dat vedením.
7. Opatření ke zmírnění rizik: Transparentní informování zaměstnanců, omezený přístup k údajům, oddělení údajů o výkonnosti a osobní identifikace.
8. Závěr a doporučení: AI může být použita za dodržení zásad proporcionality, zaměstnanci musí být poučeni a pravidelně informováni.
9. Datum a osoba odpovědná za vypracování: 2025-04-16, Ing. Petra Malá – vedoucí výroby

Přehled klíčových webových stránek

a oficiálních zdrojů, které se zabývají problematikou umělé inteligence (AI) a jejího vztahu k ochraně osobních údajů (GDPR) v rámci Evropské unie:

Oficiální instituce EU

1. **Evropská komise – Evropský přístup k umělé inteligenci**
 - a. Přehled strategií EU pro důvěryhodnou a lidsky orientovanou AI.
 - b. digital-strategy.ec.europa.eu/cs/policies/european-approach-artificial-intelligence

2. **Evropská komise – Otázky a odpovědi k AI Act**
 - a. Vysvětlení základních principů a cílů nařízení o AI.
 - b. ec.europa.eu/commission/presscorner/detail/cs/qanda_21_1683

3. **Evropský sbor pro ochranu osobních údajů (EDPB) – Umělá inteligence**
 - a. Stanoviska a doporučení k ochraně údajů v kontextu AI.
 - b. www.edpb.europa.eu/our-work-tools/our-documents/topic/artificial-intelligence_en

4. **Agentura Evropské unie pro základní práva (FRA) – Umělá inteligence a základní práva**
 - a. Zpráva o dopadech AI na lidská práva a ochranu údajů.
 - b. fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

Odborné a informační portály

1. **GDPR.cz – Generativní AI a rizika pro ochranu údajů**
 - a. Analýza rizik spojených s generativní AI a doporučení pro prevenci.
 - b. www.gdpr.cz/generativni-ai-rizika-pro-ochranu-udaju-a-jak-jim-predchazet

2. **Consentmanager – Může být AI v souladu s GDPR?**
 - a. Rady a tipy pro zajištění souladu AI systémů s GDPR.
 - b. www.consentmanager.cz/znalost/ki-gdpr

Nařízení EU a Pakt AI.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2024/1689

ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)

https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng?utm_source=chatgpt.com

Pakt AI

Zákon o AI vstoupil v platnost 1. srpna 2024. Některá ustanovení zákona o AI jsou již plně použitelná. Některé požadavky na vysoce rizikové systémy umělé inteligence a další ustanovení však budou platit až na konci přechodného období [tj. doby mezi vstupem v platnost a datem použitelnosti].

V této souvislosti Komise prosazuje Pakt o umělé inteligenci s cílem pomoci zúčastněným stranám připravit se na provádění zákona o umělé inteligenci. Pakt AI je strukturován kolem dvou pilířů.

<https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-What-is-the-AI-Pact?>

Umělá inteligence

Umělá inteligence neboli AI označuje technologie naprogramované tak, aby analyzovaly svět kolem sebe a podnikly kroky k dosažení konkrétních cílů.

<https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence>

Evropský úřad pro umělou inteligenci

Evropský úřad pro umělou inteligenci je centrem odborných znalostí o umělé inteligenci v celé EU. Hraje klíčovou roli při provádění zákona o AI – zejména pro AI pro všeobecné účely – podporuje rozvoj a používání důvěryhodné AI a mezinárodní spolupráci.

<https://digital-strategy.ec.europa.eu/en/policies/ai-office>